

PATENT COOPERATION TREATY

PCT

INTERNATIONAL PRELIMINARY REPORT ON PATENTABILITY


(Chapter II of the Patent Cooperation Treaty)

(PCT Article 36 and Rule 70)

REC'D 23 JAN 2006

WIPO

PCT

Applicant's or agent's file reference 21345_077WO1	FOR FURTHER ACTION		See Form PCT/IPEA/416
International application No. PCT/EP2004/052445	International filing date (day/month/year) 05.10.2004	Priority date (day/month/year) 06.10.2003	
International Patent Classification (IPC) or national classification and IPC H04N7/167, H04L9/30			
Applicant CANAL+ TECHNOLOGIES			
<p>1. This report is the international preliminary examination report, established by this International Preliminary Examining Authority under Article 35 and transmitted to the applicant according to Article 36.</p> <p>2. This REPORT consists of a total of 4 sheets, including this cover sheet.</p> <p>3. This report is also accompanied by ANNEXES, comprising:</p> <p>a. <input checked="" type="checkbox"/> sent to the applicant and to the International Bureau) a total of 22 sheets, as follows:</p> <p><input checked="" type="checkbox"/> sheets of the description, claims and/or drawings which have been amended and are the basis of this report and/or sheets containing rectifications authorized by this Authority (see Rule 70.16 and Section 607 of the Administrative Instructions).</p> <p><input type="checkbox"/> sheets which supersede earlier sheets, but which this Authority considers contain an amendment that goes beyond the disclosure in the international application as filed, as indicated in item 4 of Box No. I and the Supplemental Box.</p> <p>b. <input type="checkbox"/> (sent to the International Bureau only) a total of (indicate type and number of electronic carrier(s)) , containing a sequence listing and/or tables related thereto, in computer readable form only, as indicated in the Supplemental Box Relating to Sequence Listing (see Section 802 of the Administrative Instructions).</p>			
<p>4. This report contains indications relating to the following items:</p> <p><input checked="" type="checkbox"/> Box No. I Basis of the opinion</p> <p><input type="checkbox"/> Box No. II Priority</p> <p><input type="checkbox"/> Box No. III Non-establishment of opinion with regard to novelty, inventive step and industrial applicability</p> <p><input type="checkbox"/> Box No. IV Lack of unity of invention</p> <p><input checked="" type="checkbox"/> Box No. V Reasoned statement under Article 35(2) with regard to novelty, inventive step or industrial applicability; citations and explanations supporting such statement</p> <p><input type="checkbox"/> Box No. VI Certain documents cited</p> <p><input type="checkbox"/> Box No. VII Certain defects in the international application</p> <p><input type="checkbox"/> Box No. VIII Certain observations on the international application</p>			
Date of submission of the demand 14.04.2005		Date of completion of this report 19.01.2006	
Name and mailing address of the international preliminary examining authority:  European Patent Office - Gitschiner Str. 103 D-10958 Berlin Tel. +49 30 25901 - 0 Fax: +49 30 25901 - 840		Authorized Officer Bertrand, F Telephone No. +49 30 25901-406	



**INTERNATIONAL PRELIMINARY REPORT
ON PATENTABILITY**

International application No.
PCT/EP2004/052445

Box No. I Basis of the report

1. With regard to the **language**, this report is based on the international application in the language in which it was filed, unless otherwise indicated under this item.
- ☐ This report is based on translations from the original language into the following language , which is the language of a translation furnished for the purposes of:
- ☐ international search (under Rules 12.3 and 23.1(b))
 - ☐ publication of the international application (under Rule 12.4)
 - ☐ international preliminary examination (under Rules 55.2 and/or 55.3)
2. With regard to the **elements*** of the international application, this report is based on *(replacement sheets which have been furnished to the receiving Office in response to an invitation under Article 14 are referred to in this report as "originally filed" and are not annexed to this report)*:

Description, Pages

1-4	as originally filed
5-21	received on 14.04.2005 with letter of 04.04.2005

Claims, Numbers

1-20	received on 14.04.2005 with letter of 04.04.2005
------	--

Drawings, Sheets

1/6-6/6	as originally filed
---------	---------------------

- ☐ a sequence listing and/or any related table(s) - see Supplemental Box Relating to Sequence Listing

3. ☒ The amendments have resulted in the cancellation of:

- ☐ the description, pages
- ☒ the claims, Nos. 21-22
- ☐ the drawings, sheets/figs
- ☐ the sequence listing (*specify*):
- ☐ any table(s) related to sequence listing (*specify*):

4. ☐ This report has been established as if (some of) the amendments annexed to this report and listed below had not been made, since they have been considered to go beyond the disclosure as filed, as indicated in the Supplemental Box (Rule 70.2(c)).

- ☐ the description, pages
- ☐ the claims, Nos.
- ☐ the drawings, sheets/figs
- ☐ the sequence listing (*specify*):
- ☐ any table(s) related to sequence listing (*specify*):

* If item 4 applies, some or all of these sheets may be marked "superseded."

**INTERNATIONAL PRELIMINARY REPORT
ON PATENTABILITY**

International application No.
PCT/EP2004/052445

Box No. V Reasoned statement under Article 35(2) with regard to novelty, inventive step or industrial applicability; citations and explanations supporting such statement

1. Statement

Novelty (N)	Yes: Claims	1-20
	No: Claims	
Inventive step (IS)	Yes: Claims	1-20
	No: Claims	
Industrial applicability (IA)	Yes: Claims	1-20
	No: Claims	

2. Citations and explanations (Rule 70.7):

see separate sheet

**INTERNATIONAL PRELIMINARY
REPORT ON PATENTABILITY
(SEPARATE SHEET)**

International application No.

PCT/EP2004/052445

Re Item V

**Reasoned statement with regard to novelty, inventive step or industrial applicability;
citations and explanations supporting such statement**

Reference is made to the following document

D1: WO 99/43120 A (DIGITAL VIDEO EXPRESS L P ;KRAVITZ DAVID W (US);
GOLDSCHLAG DAVID) 26 August 1999 (1999-08-26)

D1 does provide a pairing system of a sink and a CAM.

The subject-matter of claim 1 is new (Article 33(2) PCT) because it shows "a combination of the first key and the second key is congruent to a pairing system key that enables...". It also involves an inventive step (Article 33(3) PCT) because in order to decrypt the broadcasted encrypted control data , the first key assigned to the decoder and the second key assigned to the portable security module are combined to obtain a key congruent to a pairing system key that enables to decrypt the broadcasted encrypted control data. In contrast, D1 does not provide a decryption key by combining the CAM ID and the sink ID.

The amendments provided together with the letter dated 04-04-2005 under Article 19(1) do not introduce subject-matter which extends beyond the content of the application as filed, contrary to Article 19(2) PCT, because they are supported by paragraphs 2, 4 and 51 as initially filed.

F.Bertrand

14. 04. 2005

(42)

REPLACEMENT SHEET

decryption using the second secret serial number SSN_{1i} and outputs a partially decrypted key. The partially decrypted key is transmitted to a decoder 112_i. The key is fully decrypted using the first secret serial number SSN_{0i} stored in SSN₀ memory 113_i. The fully decrypted key is used to descramble the scrambled audiovisual information.

[0016] The third pairing method provides a robust pairing since the second secret serial key SSN_{1i} is stored into the portable security module 110_i and is thus rendered difficult to read.

Summary of Invention

[0017] In a first aspect, the invention provides a method for pairing a decoder and a portable security module. The first element and the second element form a first decoding system among a plurality of receiving decoding systems in a broadcasting network, each receiving decoding system being adapted to descramble scrambled audiovisual information received over the broadcasting network. The method comprises selecting a first key, the first key being unique in the broadcasting network, and determining a second key according to the first key, such that a combination of the first key and the second key is congruent to a pairing system key that enables to decrypt broadcasted encrypted control data that is received to be decrypted by each receiving decoding system, the encrypted control data being identical for each receiving decoding system. The first key and the second key are respectively assigned to the decoder and the portable security module.

[0018] In a first preferred embodiment, the control data enables to descramble the scrambled audiovisual information. Furthermore, the method further comprises receiving at the first decoding system the encrypted control data, and using the first key at the decoder and using the second key at the portable security module to decrypt the encrypted control data.

REPLACEMENT SHEET

- [0019]** In a second preferred embodiment, the control data is a control word, and the audiovisual information is scrambled using the control word.
- [0020]** In a third preferred embodiment, the control data is an Entitlement Control Message (ECM) comprising a control word. The audiovisual information is scrambled using the control word.
- [0021]** In a fourth preferred embodiment, the control data is an exploitation key. The exploitation key enables to decode a control word, and the audiovisual information is scrambled using the control word.
- [0022]** In a fifth preferred embodiment, the control data is an Entitlement Management Message (EMM) comprising an exploitation key enabling to decode a control word. The audiovisual information is scrambled using the control word.
- [0023]** In a sixth preferred embodiment, the encrypted control data is decrypted using a RSA algorithm. A first prime number p and a second prime number q are selected, and a modulus number n calculated as being equal to a product of the first prime number p and the second prime number q . An encrypting key e is selected as being smaller to the modulus number and as being prime with a function of the first prime number p and the second prime number q . A private key is determined as being equal to an inverse of the encrypting key modulus the function of the first prime number p and the second prime number q . The first key and the second key are selected such that a product of the first key and the second key equals the private key modulo the function of the first prime number p and the second prime number q . The first prime number p and the second prime number q are erased.
- [0024]** In a seventh preferred embodiment, the method further comprises receiving at each receiving decoding system a message comprising the encrypted control data, and decrypting the encrypted control data using the first key at the decoder and the second key at the portable security module.

REPLACEMENT SHEET

- [0025] In an eight preferred embodiment, the encrypted control data is decrypted using a discrete logarithms algorithm. The method further comprises selecting a prime number q , selecting a primitive root of the prime number g ; wherein a product of the first key and the second key equals a private key modulo the prime number.
- [0026] In a ninth preferred embodiment, the method further comprises receiving at each receiving decoding system a message comprising an encrypted information encrypted with a session key, the message also comprising the primitive root of the prime number g power a random number k . The first key is used at the decoder and the second key is used at the portable security module to calculate the session key from the prime number power the random number k . The encrypted information is decrypted using the session key.
- [0027] In a tenth preferred embodiment, the encrypted information is the scrambled audiovisual information.
- [0028] In an eleventh preferred embodiment, the encrypted information is a control word, the audiovisual information being scrambled using the control word.
- [0029] In a twelfth preferred embodiment, the method further comprises respectively attributing the first key and the second key at least to a third element and a fourth element, the third element and the fourth element forming a second decoding system distinct from the first decoding system.
- [0030] In a second aspect the invention provides a first decoding system among a plurality of receiving decoding systems in a broadcasting network, each receiving decoding system being adapted to descramble scrambled audiovisual information received over the broadcasting network. The first decoding system comprises a decoder to which is assigned a first key, the first key being unique in the broadcasting network, and a portable security module to which is assigned a second key, the second key being determined according to the first key such that a

REPLACEMENT SHEET

combination of the first key and the second key is congruent to a pairing system that enables to decrypt broadcasted encrypted control data that is received to be decrypted by each receiving decoding system, the encrypted control data being identical for each receiving decoding system.

[0031] In a fourteenth preferred embodiment, the first decoding system further comprises receiving means to receive the broadcasted encrypted control data, and a pair of decryptions comprising a first decryption and a second decryption respectively located in the decoder and the portable security module, the pair of decryptions enabling to decrypt the broadcasted encrypted control data using the first key and the second key.

[0032] In a fifteenth preferred embodiment, the broadcasted encrypted control data is decrypted using a discrete logarithm algorithm.

[0033] In a sixteenth preferred embodiment, the broadcasted encrypted control data is decrypted using a RSA algorithm.

[0034] In a seventeenth preferred embodiment, the control data is a control word, the audiovisual information being scrambled using the control word.

[0035] In an eighteenth preferred embodiment, the control data is an exploitation key, the exploitation key enabling to decode a control word, the audiovisual information being scrambled using the control word.

[0036] In a third aspect, the invention provides an apparatus for pairing a decoder and a portable security module, the decoder and the portable security module forming a first decoding system among a plurality of receiving decoding systems in a broadcasting network, each receiving decoding system being adapted to descramble scrambled audiovisual information received over the broadcasting network. The apparatus comprises selecting means to select a first key, the first key being unique in the broadcasting network. Processing means determine a

REPLACEMENT SHEET

second key according to the first key such that a combination of the first key and the second key is congruent to a pairing system key that enables to decrypt broadcasted encrypted control data that is received at each receiving decoding system to be decrypted, the encrypted control data being identical for each receiving decoding system. Assigning means respectively assign the first key and the second key to the decoder and to the portable security module.

[0037] Other aspects and advantages of the invention will be apparent from the following description and the appended claims.

Brief Description of Drawings

[0038] FIG. 1 contains a schematic diagram of a third pairing method from prior art.

[0039] FIG. 2 shows a flowchart of a pairing method according to the invention.

[0040] FIG. 3 contains a schematic diagram of a pairing method according to the invention.

[0041] FIG. 4 contains a schematic diagram of a first embodiment of the present invention.

[0042] FIG. 5 contains a schematic diagram of a fourth embodiment of the present invention.

[0043] FIG. 6 contains a schematic diagram of a fifth embodiment of the present invention.

Detailed Description

[0044] The broadcasting network may comprise a high number of receiving decoding systems, typically several millions. The third pairing method requires the encoding system to transmit the series of twice-encrypted keys. Each twice-encrypted key is unique for a receiving decoding system or for a group of

REPLACEMENT SHEET

receiving decoding system. Hence a duration of the transmission of the series of twice-encrypted keys may be relatively long. The transmission of the series of twice-encrypted keys described in the third method occurs once a month only. There is a need for a method allowing to transmit a single encrypted key to the plurality of decoding systems of the broadcasting network, in order to provide a more frequent checking of the pairing.

[0045] FIG. 2 provides a flowchart of an example method for pairing a first element and a second element. The first element and the second element form a first decoding system among a plurality of receiving decoding systems in a broadcasting network. Each receiving decoding system is adapted to descramble scrambled audiovisual information received over the broadcasting network. A first key is selected 201. The first key is unique in the broadcasting network. A second key is determined 202 according to the first key such that a combination of the first key and the second key enables to decrypt broadcasted encrypted control data. The broadcasted encrypted control data is received to be decrypted by each receiving decoding system. The encrypted control data is identical for each receiving decoding system. The first key and the second key are assigned 203 respectively to the first element and to the second element. The first key and the second key may for example be stored respectively in a first secured memory of the first element and a second secured memory of the second element, the secured memories being protected from reading.

[0046] FIG. 3 provides an illustration of a first decoding system 301_i according to the invention among a plurality of receiving decoding systems (301₁, ..., 301_i, ..., 301_n). Each receiving decoding system is adapted to descramble scrambled audiovisual information. The first decoding system 301_i comprises a first element 302_i and a second element 303_i.

REPLACEMENT SHEET

- [0047] The first element 302_i may be a decoder, and the second element 303_i may be a portable security module. The portable security module may for example be a smartcard.
- [0048] A first key K_{i1} is assigned to the decoder and a second key K_{i2} is assigned to the smartcard. The first key K_{i1} and the second key K_{i2} form a pair of keys that is unique for the broadcasting network. Only one of the keys of the pair of keys may be randomly chosen. If the first key K_{i1} is randomly chosen, the second key K_{i2} is determined according to the first key K_{i1} such that a combination of the first key K_{i1} and the second key K_{i2} enables to decrypt broadcasted encrypted control data 304.
- [0049] The broadcasted encrypted control data 304 is intended to be decrypted by each receiving decoding system. The encrypted control data 304 is identical for each receiving decoding system (301₁, ..., 301_i, ..., 301_n). Typically, a sum of the first key K_{i1} and the second key K_{i2} , or a product of the first key K_{i1} and the second key K_{i2} , is congruent to a pairing system key K_{PS} . The pairing system key K_{PS} enables to decrypt the broadcasted encrypted control data 304. The control data are encrypted using a single encoding key K_e at an encoding system 305.
- [0050] If the broadcasted control data are encrypted and decrypted using an asymmetric cryptography algorithm, the pairing system key K_{PS} may be a private key and the encoding key K_e may be the corresponding public key. If the cryptography algorithm is symmetric, the pairing system key K_{PS} and the encoding key K_e may be identical.
- [0051] In the third pairing method from prior art, a twice-encrypted key is transmitted for each pair of secret serial number (SSN0_i, SSN1_i), i.e. for each receiving decoding system or for each group of receiving decoding systems. The encoding system has to transmit a series of twice-encrypted keys, which may be relatively long. The method according to the invention allows to transmit a single

REPLACEMENT SHEET

broadcasted encrypted data to the broadcasting network. For a single pairing system key K_{PS} corresponding to a single encoding key K_e , a wide number of distinct pairs of keys (K_{i1} , K_{i2}) may indeed be provided such that the product of the first key K_{i1} and the second key K_{i2} , is congruent to the pairing system key K_{PS} . The method according to the invention allows to test a pairing of each receiving system by transmitting a single broadcasted encrypted control data. The test of the pairing of each receiving system of the broadcasting network may be performed much more often than once a month, e.g. every 10 seconds, thus providing a more secure pairing.

- [0052] The test of the pairing may be performed by transmitting to the broadcasting network an encrypted control data that is necessary for descrambling the scrambled audiovisual information. For example, the control data may be a control word, the control word directly allowing to descramble the scrambled audiovisual information.
- [0053] The encrypted control data may also be an Entitlement Control Message (ECM) comprising the encrypted control word.
- [0054] The control data may also be an exploitation key, the exploitation key allowing to decode an encoded control word. The scrambled audiovisual information may be descrambled using the control word.
- [0055] The encrypted control data may also be an Entitlement Management Message (EMM) comprising the encrypted exploitation key.
- [0056] The encrypted control data may also be the scrambled audiovisual information, that is directly descrambled using the first key and the second key. In this latter case, the portable security module may be relatively powerful so as to be able to provide a real-time decoding.

REPLACEMENT SHEET

- [0057] If the decoder and the smartcard are paired, the combination the first key K_{i1} and the second key K_{i2} is congruent to the pairing system key K_{PS} . The decoding system receives the control data, e.g. a control word, encrypted with the encoding key K_e . The control word is decrypted using the first key at the decoder and the second key at the smartcard. The control word enables to descramble the scrambled audiovisual information at the decoder.
- [0058] If the decoder and the smartcard are not paired, the combination the first key K_{i1} and the second key K_{i2} is not congruent to the pairing system key K_{PS} . The decoding system is not able to decrypt correctly the encrypted control word and the scrambled audiovisual information is not descrambled.
- [0059] In a first embodiment, the pair of keys attached to the decoding system is attributed at least to a second receiving decoding system distinct from the first decoding system. FIG. 4 provides an illustration of the first embodiment. A "group" 401_i of decoding system ($402_{i1}, \dots, 402_{mi}$) having a same pair of keys (K_{i1}, K_{i2}) may be defined among a plurality of groups ($401_1, \dots, 401_i, \dots, 401_n$) of receiving decoding systems ($402_{11}, \dots, 402_{m1}, \dots, 402_{i1}, \dots, 402_{mi}, \dots, 402_{1n}, \dots, 402_{mn}$). This embodiment may render the pairing easier to perform, but the pairing is tested the same way as described above. An encoding system 403 encrypt a control data, and the encrypted control data 404 is broadcasted over the network. Each receiving system ($402_{11}, \dots, 402_{m1}, \dots, 402_{i1}, \dots, 402_{mi}, \dots, 402_{1n}, \dots, 402_{mn}$) of any group receives the broadcasted encrypted control data 404 and decrypt the control data using the first key and the second key. In this embodiment, a decoder from a determined group may operate with any smartcard of the determined group. Each group comprises a relatively low number of receiving decoding elements, so that a smartcard of a first person has a relatively low probability to be able to operate with a decoder of a second person.

REPLACEMENT SHEET

- [0060] In a second embodiment, the pairing is performed at a beginning of a subscription. An operator downloads the first key and the second key respectively into the decoder and the smartcard. The first key and the second key are protected from reading.
- [0061] In a third embodiment, the first key and the second key are regularly replaced, e.g. once a month. A decoder group key $G1$ is attached to the decoder and a smartcard group key $G2$ may be attached to the smartcard. The decoder group key $G1$ and the smartcard group key $G2$ may be for example a serial number respectively attached to a single decoder and a single smartcard. The decoder group key $G1$ and the smartcard group key $G2$ may also be respectively attached to a group of decoders or to a group of smartcards. The decoder group key $G1$ and the smartcard group key $G2$ form a set of keys that is specific to the first decoding system or to a group of receiving decoding system.
- [0062] The pairing is regularly performed: a first EMM and a second EMM are sent to the first decoding system. The decoder receives the first EMM and the second EMM, and transmits the second EMM to the smartcard. The first EMM contains the first key d_1 encoded with the decoder group key $G1$. The second EMM contains the second key d_2 encoded with the smartcard group key $G2$. The first key d_1 and the second key d_2 are selected such that the product of the first key d_1 and the second key d_2 is congruent to the pairing system key K_{PS} . The decoder decodes the first key d_1 with the decoder group key $G1$ and the smartcard decodes the second key d_2 with the smartcard group key $G2$.
- [0063] The first key d_1 and the second key d_2 allow to decrypt broadcast encrypted control data, e.g. the control word encrypted with the encoding key. The encoding key K_e and the pairing system key K_{PS} may also be changed every month and the first key d_1 and the second key d_2 may be determined from the new values of the encoding key K_e and the pairing system key K_{PS} . If a person

REPLACEMENT SHEET

once determines values of two pairs of keys, the person may be able to use a first decoder from a first decoding device with a second smartcard from another receiving decoding system. However, one month later, when the first key d_1 and the second key d_2 are replaced, the person may have to determine the new values of two pairs of keys. This third alternative embodiments adds more security to the pairing system.

[0064] RSA algorithm

[0065] In a fourth embodiment, the control data is encrypted using a RSA algorithm. FIG. 5 provides a flowchart illustrating the fourth embodiment. The pairing is performed by first selecting a first prime number p and a second prime number q . A modulus number n is calculated as being equal to a product of the first prime number p and the second prime number q :

[0066] $n = p * q$

[0067] An encoding key K_e is then selected from the values of the first prime number p , the second prime number q and the modulus number n , such that:

[0068] $K_e < n$ and K_e is prime with $\phi(p, q)$,

[0069] wherein $\phi(p, q)$ is a function of the first prime number p and the second prime number q such that:

[0070] $\phi(p, q) = (p-1)(q-1)$

[0071] The RSA algorithm is an asymmetric cryptography algorithm. The encoding key K_e is intended to encrypt a control word CW at an encoding system 501. The encoding key K_e is a public key and a pairing system key K_{PS} corresponding to the encoding key K_e may be determined, the pairing system key K_{PS} being a private key distinct from the public key. The pairing system key K_{PS} may be determined as follows:

[0072] $K_{PS} = (1 / K_e) \text{ modulo } \phi(p, q)$

REPLACEMENT SHEET

- [0073] A pair of keys comprising a first key d_1 and a second key d_2 is selected such that a product of the first key d_1 and the second key d_2 is congruent to the pairing system key K_{PS} :
- [0074] $K_{PS} = d_1 * d_2 \text{ modulo } \varphi(p, q)$
- [0075] The first key may be randomly selected first, and the second key may be determined according to the first key d_1 , the pairing system key K_{PS} and the function $\varphi(p, q)$.
- [0076] The first prime number p and the second prime number q are not assigned to any apparatus; they are erased so that a person knowing the encoding key K_e and the modulus number n may not be able to decrypt data encrypted with the encoding key K_e . The first prime number p and the second prime number q are indeed necessary for determining the pairing system key K_{PS} .
- [0077] The first key may be assigned to a decoder 502, and the second key may be assigned to a smartcard 503. The decoder 502 and the smartcard 503 form a first decoding system 504 among a plurality of receiving decoding systems of a broadcasting network. For each receiving decoding system a distinct pair of keys may be provided.
- [0078] The pairing is periodically tested. The audiovisual information m is scrambled 505 using the control word CW at the encoding system 501 and continuously transmitted to the plurality of receiving decoding systems. The control word changes every 10 seconds or so.
- [0079] The encoding system 501 encrypts 506 the control word CW using the encoding key K_e and transmits the encrypted control word to the plurality of receiving decoding systems.
- [0080] The decoding system 504 receives both the scrambled audiovisual information $E_{CW}(m)$ and the encrypted control word $E_{K_e}(CW)$. The encrypted

REPLACEMENT SHEET

control word $E_{K_e}(CW)$ may be received at the decoder 502 and may for example be transmitted to the smartcard 503. The smartcard may calculate a first intermediate value $[E_{K_e}(CW)]^{d_2}$ being equal or congruent to the encrypted control word $E_{K_e}(CW)$ power the second key d_2 and transmit it to the decoder 502. The decoder may receive the first intermediate value $[E_{K_e}(CW)]^{d_2}$. A second intermediate value $[[E_{K_e}(CW)]^{d_2}]^{d_1}$ may be calculated at the decoder as being equal to the first intermediate value $[E_{K_e}(CW)]^{d_2}$ power the first key d_1 . The control word CW is equal to the second intermediate value modulo the modulus number n .

[0081] The control word is thus decrypted using the first key at the decoder and using the second key at the smartcard. The scrambled audiovisual information $E_{CW}(m)$ may be descrambled 507 using the control word CW . If the decoder and the smartcard are not correctly paired, i.e. the product of the first key d_1 assigned to the decoder and the second key d_2 assigned to the smartcard is not congruent to the pairing system key K_{PS} , the control word CW is not decrypted and the scrambled audiovisual information is not descrambled.

[0082] If a person knows a first pair of keys (d_{11}, d_{21}) attributed to a first decoding system, the person is not able in this embodiment to generate all the pairs of keys. Indeed, the function $\varphi(p, q)$ has been erased, and the function $\varphi(p, q)$ is necessary for determining a pair of keys since the product of the first key d_{11} and the second key d_{21} equals the pairing system key K_{PS} modulo the function $\varphi(p, q)$. It is necessary to also know a second pair of keys (d_{21}, d_{22}) to determine the function $\varphi(p, q)$. The function $\varphi(p, q)$ indeed divides a difference $d_{21} * d_{22} - d_{11} * d_{12}$.

[0083] In a first alternative embodiment, the decoder receives the encrypted control word $E_{K_e}(CW)$ and performs a first operation: a first alternative intermediate value $[E_{K_e}(CW)]^{d_1}$ is calculated as being equal or congruent to the encrypted

REPLACEMENT SHEET

control word $E_{K_e}(CW)$ power the first key d_1 . The first alternative intermediate value $[E_{K_e}(CW)]^{d_1}$ is transmitted to the smartcard. The second intermediate value $[[E_{K_e}(CW)]^{d_2}]^{d_1}$ may be calculated at the smartcard as being equal to the first alternative intermediate value $[E_{K_e}(CW)]^{d_1}$ power the second key d_2 . The control word CW is determined from the second intermediate value $[[E_{K_e}(CW)]^{d_2}]^{d_1}$ and used to descramble the scrambled audiovisual information $E_{CW}(m)$.

[0084] In a second alternative embodiment, the first intermediate value is not directly transmitted from the smartcard to the decoder (or from the decoder to the smartcard). The first intermediate value is encoded using a secret key known only by the decoder and the smartcard before being transmitted. An asymmetric cryptography algorithm may also be used for the communication from the smartcard to the decoder.

[0085] In a third alternative embodiment, the encoding key K_e and the pair of keys are not directly used for encrypting and decrypting the control word, but an exploitation key. The exploitation key itself allows to encode and decode the control word, the control word allowing to descramble the scrambled audiovisual information. In this third alternative embodiment, the test of the pairing may occur less frequently, e.g. once a month.

[0086] **Discrete logarithm algorithm**

[0087] In a fifth embodiment, the broadcasted data is encrypted using a discrete logarithm algorithm. FIG. 6 provides a flowchart illustrating the fifth embodiment. The pairing is performed by first selecting a prime number q and a primitive root g of the prime number q . A private key a for communication between an encoding system 601 and any receiving decoding system of a plurality of receiving decoding systems (not represented) is selected and a session key g^{ka} is calculated as being equal to the primitive root g power a

REPLACEMENT SHEET

product of the private key a and a random number k , wherein the random number is randomly chosen.

- [0088] A first key a_1 is selected. A second key a_2 is determined according to the first key a_1 , the prime number q and the private key a , such that the product of the first key a_1 and the second key a_2 is congruent to the private key a modulo the prime number q . The first key a_1 and the second key a_2 form a pair of keys that is unique in a broadcasting network.
- [0089] The pairing is periodically tested. The encoding system 601 picks 602 a value of the random number k . An information is encrypted 603 using the session key. The encoding system 601 transmits to the broadcasting network a message. The message comprises the encrypted information $E_g(m)$ and a partial key g^k , the partial key being equal to the primitive root g power the random number k . A decoder 604 receives and transmits to a smartcard 605 the partial key.
- [0090] The first key a_1 and the second key a_2 are used to decrypt the encrypted information. The smartcard calculates a first intermediate value $[g^k]^{a_2}$, as being equal or congruent to the partial key g^k power the second key a_2 . The first intermediate value $[g^k]^{a_2}$ is then transmitted to the decoder. The decoder calculates a second intermediate value $[[g^k]^{a_2}]^{a_1}$ as being equal to the first intermediate value $[g^k]^{a_2}$ power the first key a_1 . The session key may be determined from the second intermediate value as being equal to the second intermediate value modulo the prime number q .
- [0091] The encrypted information may be decrypted using the session key.
- [0092] The information may be an audiovisual information. In this latter case, the first key a_1 and the second key a_2 are used to decrypt the encrypted audiovisual information via the session key. The pairing test may occurs frequently, e.g. every 10 seconds.

REPLACEMENT SHEET

- [0093] In a first alternative embodiment, the encrypted information is an encrypted control word, the control word being used to descramble audiovisual information. The first key a_1 and the second key a_2 are used to decrypt the control word via the session key. The control word enables to descramble the audiovisual information.
- [0094] In a second alternative embodiment, the decoder receives the partial key g^k and performs a first operation: a first alternative intermediate value $[g^k]^{a_1}$ is calculated as being equal or congruent to the partial key g^k power the first key a_1 . The first alternative intermediate value $[g^k]^{a_1}$ is transmitted to the smartcard. The second intermediate value $[[g^k]^{a_2}]^{a_1}$ may be calculated at the smartcard as being equal to the first alternative intermediate value $[g^k]^{a_1}$ power the second key a_2 . The session key g^{ka} is determined from the second intermediate value $[[g^k]^{a_2}]^{a_1}$ and used to descramble the encrypted information $E_g(m)$.
- [0095] In a third alternative embodiment, the communicating between the decoder and the smartcard may be encoded with a secret key that is common to the decoder and the smartcard.
- [0096] In order to increase the security of the system, any or all of the above described embodiments may be implemented in combination with each other.
- [0097] The present invention is particularly applicable to the transmission of a television broadcast. The present invention also extends to a decoder and security module adapted for descrambling scrambled audiovisual information as described above.
- [0098] The term "portable security module" is used to mean any conventional chip-based portable card type devices possessing, for example, microprocessor and/or memory storage. This may include smart cards, PCMCIA cards, SIM cards etc. Included in this term are chip devices having alternative physical forms, for example key-shaped devices such as are often used in TV decoder systems.

REPLACEMENT SHEET

[0099] The terms "scrambled" and "encrypted" and "control word" and "key" have been used here in a number of ways for the purpose of clarity of language. However, it will be understood that no fundamental distinction is to be made between "scrambled data" and "encrypted data" or between a "control word" and a "key".

[00100] The term "control data" refers to any data allowing more or less directly to decode an audiovisual information, or the audiovisual information itself.

[00101] Similarly, whilst the description refers to "receiver/decoders" and "decoders" it will be understood that the present invention applies equally to embodiments having a receiver integrated with the decoder as to a decoder unit functioning in combination with a physically separate receiver, decoder units incorporating other functionalities, and decoder units integrated with other devices, such as televisions, recording devices etc.

[00102] The terms "plurality of decoding systems", or "plurality of decoding systems in a broadcasting network" have been used to mean a high number of decoding systems corresponding to a decoding system subscriber base, typically more than one thousand.

[00103] While the invention has been described with respect to a limited number of embodiments, those skilled in the art, having benefit of this disclosure, will appreciate that other embodiments can be devised which do not depart from the scope of the invention as disclosed herein. Accordingly, the scope of the invention should be limited only by the attached claims.

EPO - DG 1

REPLACEMENT SHEET

14. 04. 2005

Claims

(42)

- [c1]** A method for pairing a decoder and a portable security module, the decoder and the portable security module forming a first decoding system among a plurality of receiving decoding systems in a broadcasting network, each receiving decoding system being adapted to descramble scrambled audiovisual information received over the broadcasting network, the method comprising:
selecting a first key, the first key being unique in the broadcasting network;
assigning the first key to the decoder;
the method being characterized in that it further comprises
determining a second key according to the first key, such that a combination of the first key and the second key is congruent to a pairing system key that enables to decrypt broadcasted encrypted control data that is received to be decrypted by each receiving decoding system, the encrypted control data being identical for each receiving decoding system;
assigning the second key to the portable security module.
- [c2]** The method according to claim 1, wherein the control data enables to descramble the scrambled audiovisual information, the method further comprising:
receiving at the first decoding system the encrypted control data;
using the first key at the decoder and using the second key at the portable security module to decrypt the encrypted control data.
- [c3]** The method according to any one of claims 1 to 2, wherein the control data is a control word, the audiovisual information being scrambled using the control word.
- [c4]** The method according to any one of claims 1 to 2, wherein the control data is an Entitlement Control Message (ECM) comprising a control word, the audiovisual information being scrambled using the control word.

REPLACEMENT SHEET

- [c5] The method according to any one of claims 1 to 2, wherein the control data is an exploitation key, the exploitation key enabling to decode a control word, the audiovisual information being scrambled using the control word.
- [c6] The method according to any one of claims 1 to 2, wherein the control data is an Entitlement Management Message (EMM) comprising an exploitation key enabling to decode a control word, the audiovisual information being scrambled using the control word.
- [c7] The method according to any one of claims 1 to 6, wherein the encrypted control data is decrypted using a RSA algorithm, the method further comprising:
selecting a first prime number p and a second prime number q ;
calculating a modulus number n as being equal to a product of the first prime number p and the second prime number q ;
selecting an encrypting key e as being smaller to the modulus number and as being prime with a function of the first prime number p and the second prime number q ;
determine a private key as being equal to an inverse of the encrypting key modulus the function of the first prime number p and the second prime number q ;
selecting the first key and the second key such that a product of the first key and the second key equals the private key modulo the function of the first prime number p and the second prime number q ;
erasing the first prime number p and the second prime number q .
- [c8] The method according to claim 7, further comprising:
receiving at each receiving decoding system a message comprising the encrypted control data;
decrypting the encrypted control data using the first key at the decoder and the second key at the portable security module.

REPLACEMENT SHEET

- [c9] The method according to any one of claims 1 to 2, wherein the encrypted control data is decrypted using a discrete logarithms algorithm, the method further comprising:
selecting a prime number q ;
selecting a primitive root of the prime number g ;
and wherein a product of the first key and the second key equals a private key modulo the prime number.
- [c10] The method according to claim 9, further comprising:
receiving at each receiving decoding system a message comprising an encrypted information encrypted with a session key, the message also comprising the primitive root of the prime number g power a random number k ;
using the first key at the decoder and using the second key at the portable security module to calculate the session key from the prime number power the random number k ;
decrypting the encrypted information using the session key.
- [c11] The method according to claim 10, wherein the encrypted information is the scrambled audiovisual information.
- [c12] The method according to claim 10, wherein the encrypted information is a control word, the audiovisual information being scrambled using the control word.
- [c13] The method according to any one of claims 1 to 12, further comprising respectively attributing the first key and the second key at least to a third element and a fourth element, the third element and the fourth element forming a second decoding system distinct from the first decoding system.
- [c14] A first decoding system among a plurality of receiving decoding systems in a broadcasting network, each receiving decoding system being adapted to

REPLACEMENT SHEET

descramble scrambled audiovisual information received over the broadcasting network, the first decoding system comprising:

a decoder to which is assigned a first key, the first key being unique in the broadcasting network;

a portable security module to which is assigned a second key,

the first decoding system being characterized in that

the second key is determined according to the first key such that a combination of the first key and the second key is congruent to a pairing system that enables to decrypt broadcasted encrypted control data that is received to be decrypted by each receiving decoding system, the encrypted control data being identical for each receiving decoding system.

[c15] The first decoding system according to claim 14, further comprising:

receiving means to receive the broadcasted encrypted control data;

a pair of decryptions comprising a first decryption and a second decryption respectively located in the decoder and the portable security module, the pair of decryptions enabling to decrypt the broadcasted encrypted control data using the first key and the second key.

[c16] The first decoding system according to any one of claims 14 or 15, wherein the broadcasted encrypted control data is decrypted using a discrete logarithm algorithm.

[c17] The first decoding system according to any one of claims 14 or 15, wherein the broadcasted encrypted control data is decrypted using a RSA algorithm.

[c18] The first decoding system according to any one of claims 14 to 17, wherein the control data is a control word, the audiovisual information being scrambled using the control word.

REPLACEMENT SHEET

- [c19] The first decoding system according to any one of claims 14 to 17, wherein the control data is an exploitation key, the exploitation key enabling to decode a control word, the audiovisual information being scrambled using the control word.
- [c20] An apparatus for pairing a decoder and a portable security module, the decoder and the portable security module forming a first decoding system among a plurality of receiving decoding systems in a broadcasting network, each receiving decoding system being adapted to descramble scrambled audiovisual information received over the broadcasting network, the apparatus being characterized in that it comprises:
- selecting means to select a first key, the first key being unique in the broadcasting network;
 - processing means to determine a second key according to the first key such that a combination of the first key and the second key is congruent to a pairing system key that enables to decrypt broadcasted encrypted control data that is received at each receiving decoding system to be decrypted; the encrypted control data being identical for each receiving decoding system;
 - assigning means to respectively assign the first key and the second key to the decoder and to the portable security module.